

Resd PCT/JP 27.10.2004

10/5329

PCT/JP 2004/013956

21.10.2004

日 本 国 特 許 庁
JAPAN PATENT OFFICE

REC'D 11 NOV 2004

WIPO

PCT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: 2004年 2月26日

出 願 番 号
Application Number: 特願2004-050848
[ST. 10/C]: [JP2004-050848]

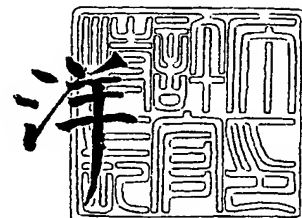
出 願 人
Applicant(s): 大日本印刷株式会社

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

2004年10月 1日

特許庁長官
Commissioner,
Japan Patent Office

小 川



BEST AVAILABLE COPY

出証番号 出証特2004-3088407

【書類名】 特許願
【整理番号】 GF600008
【提出日】 平成16年 2月26日
【あて先】 特許庁長官 殿
【国際特許分類】 G03G 21/04
【発明者】
 【住所又は居所】 東京都新宿区市谷加賀町一丁目 1 番 1 号 大日本印刷株式会社内
 【氏名】 姉川 武彦
【発明者】
 【住所又は居所】 東京都新宿区市谷加賀町一丁目 1 番 1 号 大日本印刷株式会社内
 【氏名】 矢野 義博
【特許出願人】
 【識別番号】 000002897
 【氏名又は名称】 大日本印刷株式会社
 【代表者】 北島 義俊
【代理人】
 【識別番号】 100111659
 【弁理士】
 【氏名又は名称】 金山 聡
【手数料の表示】
 【予納台帳番号】 013055
 【納付金額】 21,000円
【提出物件の目録】
 【物件名】 特許請求の範囲 1
 【物件名】 明細書 1
 【物件名】 図面 1
 【物件名】 要約書 1
 【包括委任状番号】 9808512

【書類名】特許請求の範囲**【請求項 1】**

情報記憶媒体と、前記情報記憶媒体の記憶情報を読み取り可能としたリーダライタを備えた情報処理端末と、前記情報処理端末から情報の受信を可能に接続され、前記情報処理端末から受信した情報を紙媒体に出力する出力装置と、前記出力装置と通信可能に接続されているサーバと、からなる出力情報管理システムであって、

前記情報記憶媒体は、利用者を特定可能な I D 情報が記憶され記憶手段を有し、

前記リーダライタは、前記情報記憶媒体に記憶された I D 情報を読み取る読取手段を有し

前記情報処理端末は、前記リーダライタで読み取った I D 情報と、前記出力装置で紙媒体に出力する出力情報とを前記出力装置に送信する手段とを有し、

前記出力装置は、前記情報処理端末から受信した I D 情報と出力情報とを前記サーバに送信する手段を有し、

前記サーバは、前記前記出力装置から受信した I D 情報と出力情報とを関係付けてデータベースに記憶させる手段を有することを特徴とする出力情報管理システム。

【請求項 2】

前記情報記憶媒体が、I C カードであることを特徴とする請求項 1 記載の出力情報管理システム。

【書類名】明細書

【発明の名称】出力情報管理システム

【技術分野】

【0001】

本発明は、紙媒体に情報を出力する機能を有する複写機やプリンターなどの出力装置により重要情報などが不正に紙媒体に出力されて情報の漏洩が行なわれることを防止すると共に、たとえ不正な出力が行なわれた場合でも、その情報を出力した者を特定可能とした出力情報管理システムに関する。

【背景技術】

【0002】

従来、紙媒体に情報を出力する機能を有する複写機やプリンターなどの出力装置において、第三者が出力装置を使用して、不正に重要情報を紙媒体に出力して持ち出すといった情報の漏洩が行なわれたり、使用権限を有しない第三者による出力装置の無断使用などを防止するため、正規の使用権限を有する利用者が、管理用のカード等の情報記憶媒体を所持して出力装置を使用する際にこれらの情報記憶媒体を用いて、本人照合などを行なうことで、出力装置の利用管理を行なう場合がある。

【0003】

これら管理用のカード等の情報記憶媒体を用いた利用者の制限に関する従来の技術は、既に公知となっているものがある。（例えば、特許文献1及び2、参照）

【特許文献1】特開2000-10441号公報

【特許文献2】特開2000-98833号公報

【0004】

しかしながら、これら従来の出力装置に関する使用管理では、管理用のカード等の情報記憶媒体を所持する使用権限を有する者以外の第三者による出力装置の使用を防止することはできるが、仮に、正規に出力装置の使用権限を有する者自身が、出力装置を用いて不正に重要情報を紙媒体に出力させて盗むなどの不正行為を行ったとした場合には、その不正行為を防止することはできないという問題がある。

【0005】

また、この場合には、その不正行為が行なわれたという証拠も無いことが多く、内部の者による不正行為に対してのセキュリティ上の予防が図られにくく、従来の技術ではセキュリティ効果がほとんどないという問題がある。

したがって、従来の不正防止技術では、正規に出力装置の使用権限を有する者に対しての不正防止効果はなく、不正行為を行うか否かは、正規に出力装置の使用権限を有する者のモラルを信用するしかないという状況である。

【発明の開示】

【発明が解決しようとする課題】

【0006】

本発明は、紙媒体に情報を出力する機能を有する出力装置が、使用管理用のカード等の情報記憶媒体を所持する使用権限を有する者以外の第三者により使用されることを防止すると共に、更に、正規に出力装置の使用権限を有する者により、不正に重要情報を媒体に出力させて盗むなどの不正行為が行なわれた場合でも、誰が、どのような内容の情報を出力装置で出力したのかに関して具体的な証拠が残るようにして、不正行為の事前予防と、不正行為が行なわれた場合の調査が効率的に行なえるようにした出力情報管理システムを提供する。

【課題を解決するための手段】

【0007】

本発明の出力情報管理システムは、情報記憶媒体と、前記情報記憶媒体の記憶情報を読み取り可能としたリーダーライタを備えた情報処理端末と、前記情報処理端末から情報の受信を可能に接続され、前記情報処理端末から受信した情報を紙媒体に出力する出力装置と、前記出力装置と通信可能に接続されているサーバと、からなる出力情報管理システムで

あって、前記情報記憶媒体は、利用者を特定可能なID情報が記憶され記憶手段を有し、前記リーダライタは、前記情報記憶媒体に記憶されたID情報を読み取る読取手段を有し、前記情報処理端末は、前記リーダライタで読み取ったID情報と、前記出力装置で紙媒体に出力する出力情報とを前記出力装置に送信する手段とを有し、前記出力装置は、前記情報処理端末から受信したID情報と出力情報とを前記サーバに送信する手段を有し、前記サーバは、前記前記出力装置から受信したID情報と出力情報とを関係付けてデータベースに記憶させる手段を有することを特徴とする。

【0008】

本発明の出力情報管理システムは、情報記憶媒体がICカードであることを特徴とする。

【発明の効果】**【0009】**

本発明の出力情報管理システムは、パソコンなどの情報処理端末からプリンタなどの出力装置に送信されてきた情報を出力装置により、紙媒体に出力する際に、出力装置で出力した情報と、利用者を特定可能なID情報とを関係付けてサーバ側のデータベースに記憶させておくので、正規の使用権限を有する者が不正行為を行なったとしても、誰が、どのような内容のプリント出力を行ったのかをデータベースに記憶された情報を調べることで、簡単に調査することができるという効果がある。

【発明を実施するための最良の形態】**【0010】**

以下、本発明の実施形態に係る出力情報管理システムについて、図面に基づいて詳細に説明する。

図1は、本発明の実施形態に係る出力情報管理システムの概要を説明するための図、図2は、本発明の実施形態に係る出力情報管理システムのシステムブロック図、図3及び図4は、本発明の実施形態に係る出力情報管理システムの処理手順を示すフローチャートである。

【0011】

本発明の実施形態に係る出力情報管理システムは、図1に示すように、利用者用の情報記憶媒体であるICカード1と、ICカードリーダライタ2を備えたパソコンなどの情報処理端末3と、この情報処理端末3から情報の受信を可能に接続され、情報処理端末3から受信した情報を紙媒体に出力するプリンタなどの出力装置4と、出力装置4と通信回線5を介して通信可能に接続されているサーバ6とから構成されている。

例えば、会社などの組織では、ビルのワンフロアに複数の社員が個々のデスクにパソコンを置いて仕事をし、出力装置4は共通で使用するために1台や2台が所定の場所に設置され、各自が必要に応じて、自分のパソコンから複写機でプリントするための情報を送信して、紙媒体にプリント出力している。

【0012】

本発明においても、1台の出力装置4には、複数台のパソコンなどの情報処理端末3が情報の送信可能に接続されており、1台の出力装置4を複数の使用者が共通で使用して情報のプリント出力が行えるようにシステム構成されている。

また、サーバ6は、管理センターなどに設置して、通信回線5を介して複数の出力装置4と通信可能に接続され、共通して使用可能にシステム化されている。

【0013】

ICカード1の記憶手段には、ICカード1の利用者を特定することができるID情報と、プライベート鍵と、このプライベート鍵と対として用いる公開鍵を有する電子証明書とが記憶されている。

また、出力装置4とサーバ6も、プライベート鍵と、電子証明書とをそれぞれ保持している。

ICカード1の記憶手段には、ICカード1の利用者を特定することができるID情報と、プライベート鍵と、このプライベート鍵と対として用いる公開鍵を有する電子証明書

とが記憶されている。

そして、ICカードリーダライタ2は、ICカード1に記憶されている情報を読み取り情報処理端末3に送信する情報読取手段7や、情報処理端末3からICカード1に情報を書き込む情報書込手段8を有している。

【0014】

また、図2に示すように、パソコンなどの情報処理端末3には、表示手段9、送受信手段10、入力手段11、記憶手段12、暗号化手段13、制御手段14などが備えられている。

出力装置4でプリント出力しようとする情報は、入力手段11から入力した情報でもよいし、記憶手段12に記憶させておいた情報を用いてもよいが、プリント出力しようとする情報は、セキュリティ保護のためにSSL方式で暗号化した状態で出力装置4へと送信される。

【0015】

情報処理端末3と出力装置4の間における情報の暗号化は、ICカード1と出力装置4とがそれぞれ持っている電子証明書を交換して、電子証明書を認証して、セッション鍵（共通鍵）を共有し、その後の情報の暗号化はこのセッション鍵を用いて行う。

また、暗号化された情報を送るとき、使用者のICカード1内のプライベート鍵でデジタル署名を作成して、同時に送ってもかまわない。

【0016】

また、出力装置4には、送受信手段15、暗号化手段16、復号手段17、表示手段18、操作手段19、警報音発生手段20、プリント出力手段21、記憶手段22、通信手段23、制御手段24などが備えられている。

復号手段17は、情報処理端末3から送信され、出力装置4で受信した暗号化された受信情報を、情報処理端末3が保持している出力装置のプライベート鍵により復号する機能を有している。

プリント出力手段21は、復号手段17で復号された情報を紙媒体25にプリント出力する機能を有している。

【0017】

記憶手段22には、出力装置4のプライベート鍵と、電子証明書とが記憶されている。

尚、サーバ6の記憶手段にもプライベート鍵と、電子証明書とが記憶されている。

出力装置4からサーバ6へ情報を送る際にも、SSL方式で情報を暗号化する。

ここで、出力装置4からサーバ6に送信する情報としては、情報処理端末3から出力装置4に送信されて、プリント出力手段21で紙媒体25にプリント出力された情報である。

これら一連の処理は、記憶手段22に記憶されている制御プログラムに基づいて処理される。

【0018】

次に、サーバ6には、通信手段26、記憶手段27、警告情報送信手段28、出力照合判定手段29、復号手段30、登録手段32、制御手段33、ID情報データベース34、出力禁止情報データベース35、出力情報データベース36、などが備えられている。

ID情報データベース34には、ICカード1に記憶されているID情報と、そのICカード1の使用者を特定することができる情報として、例えば、社員番号、氏名、所属部署名、役職などが関係付けられて登録されている。

出力禁止情報データベース35には、予め出力装置4からプリント出力することが禁止されている情報が登録されている。

これらの出力禁止情報は、ID情報と関係付けられた人物の職務範囲や役職などによって、その人物毎に出力が禁止される場合と、出力してもよい場合とに分かれるようにすることもできる。

【0019】

出力情報データベース36には、出力装置4でプリント出力した情報と、そのプリント

出力した人物が使用した IC カード 1 に記憶されている ID 情報とを関係付けて、出力装置 4 の使用履歴情報を登録して随時蓄積される。

したがって、出力情報データベース 36 と ID 情報データベース 34 に登録された情報から、誰が、どのような内容のプリント出力を行ったのかが調べられるようにしてある。

登録手段 32 は、出力装置 4 から送信されサーバ 6 で受信し、復号手段 30 で復号したプリント出力情報と、同時に受信した ID 情報とを関係付けて出力情報データベース 36 に登録する機能を有している。

【0020】

また、出力照合判定手段 29 は、出力装置 4 からサーバ 6 で受信したプリント出力情報が、出力禁止情報データベース 35 に登録されている出力禁止情報に該当する情報であるか否かを照合判定する機能を有している。

そして、警告情報送信手段 28 は、出力照合判定手段 29 による判定の結果において、プリント出力が禁止されていると判定された際に、サーバ 6 から出力装置 4 に対して、出力装置 4 の警報音発生手段 20 から警報音を発生させるための信号を送信する機能を有している。

記憶手段 27 には、制御プログラムが搭載され、制御手段 33 による制御方法をコントロールしている。

【0021】

次に、本発明の実施形態に係る出力情報管理システムの処理手順を、図 3 に示すフローチャートに基づいて説明する。

まず、使用に際して、IC カードリーダライタ 2 に IC カード 1 をセットし、IC カード 1 の記憶手段に記憶されている ID 情報と電子証明書とを IC カードリーダライタ 2 で読み取る。(ステップ S1)

IC カードリーダライタ 2 で読み取られたこれらの情報は、情報処理端末 3 に送られる。(ステップ S2)

【0022】

次に、情報処理端末 3 において、出力装置 4 でプリント出力する情報を特定した後に、この情報を SSL 方式で暗号化して情報処理端末 3 から出力装置 4 に送信する。(ステップ S3)

【0023】

次に、出力装置 4 では、情報処理端末 3 から受信した情報を、情報処理端末 3 と出力装置 4 で共有しているセッション鍵で復号させる。(ステップ S5)

そして、復号させた情報をプリント出力手段 21 により紙媒体 25 にプリント出力させる。(ステップ S6)

次に、紙媒体 25 にプリント出力させた情報を、SSL 方式で暗号化してサーバ 6 へ送信させる。(ステップ S7)

【0024】

サーバ 6 では、受信した情報を出力装置 4 とサーバ 6 で鍵共有しているセッション鍵で復号させる。(ステップ S9)

復号させた情報は、出力禁止情報データベース 35 に登録されている出力禁止情報に該当しないか否かが照合判定される。(ステップ S8)

この照合判定の結果、出力禁止情報に該当すると判定された場合には、警告情報送信手段 28 により、サーバ 6 から出力装置 4 に対して警告情報が送信される。(ステップ S9)

警告情報を受信した出力装置 4 では、警報音発生手段 20 により警報音を発生させて、プリント出力が禁止されている情報がプリント出力されたことを知らせる。(ステップ S10)

【0025】

また、サーバ 6 においては、出力情報データベース 36 に、復号させた情報と、IC カードリーダライタ 2 から送られてきた ID 情報とを関係付けた状態で登録させる。(ステ

ップ S11)

以上のようにして、出力装置 4 でプリント出力された情報は、全て ID 情報とを関係付けた状態で出力情報データベース 36 に登録され、プリント出力の履歴情報が蓄積される。

また、情報処理端末 3 から出力装置 4 に送信される情報や、出力装置 4 からサーバ 6 に送信される情報は、いずれも SSL 方式により保護されているのでセキュリティが確保されている。

【図面の簡単な説明】

【0026】

【図 1】本発明の実施形態に係る出力情報管理システムの概要を説明するための図である。

【図 2】本発明の実施形態に係る出力情報管理システムのシステムブロックである。

【図 3】本発明の実施形態に係る出力情報管理システムの処理手順を示すフローチャートである。

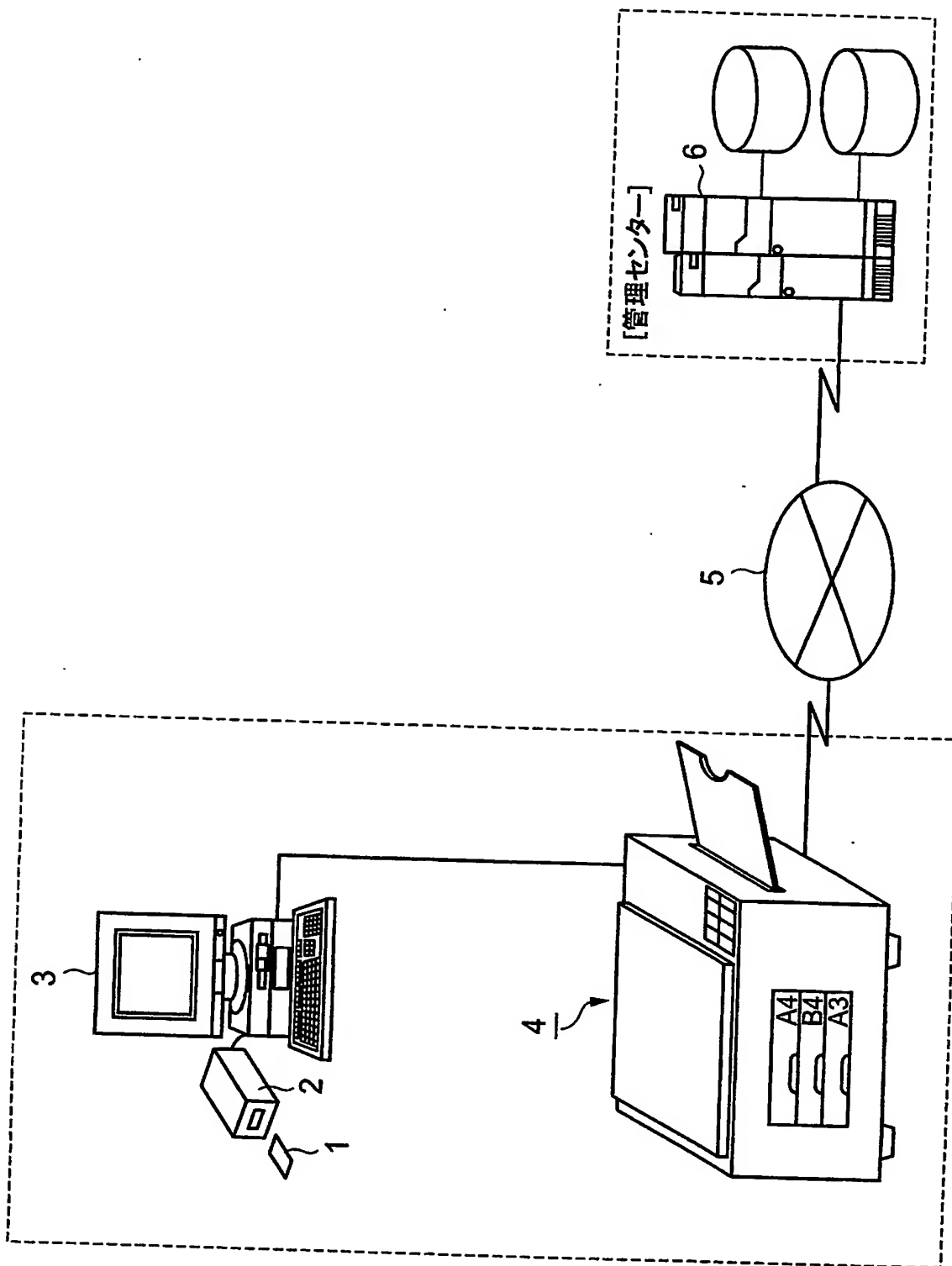
【図 4】本発明の実施形態に係る出力情報管理システムの処理手順を示すフローチャートである。

【符号の説明】

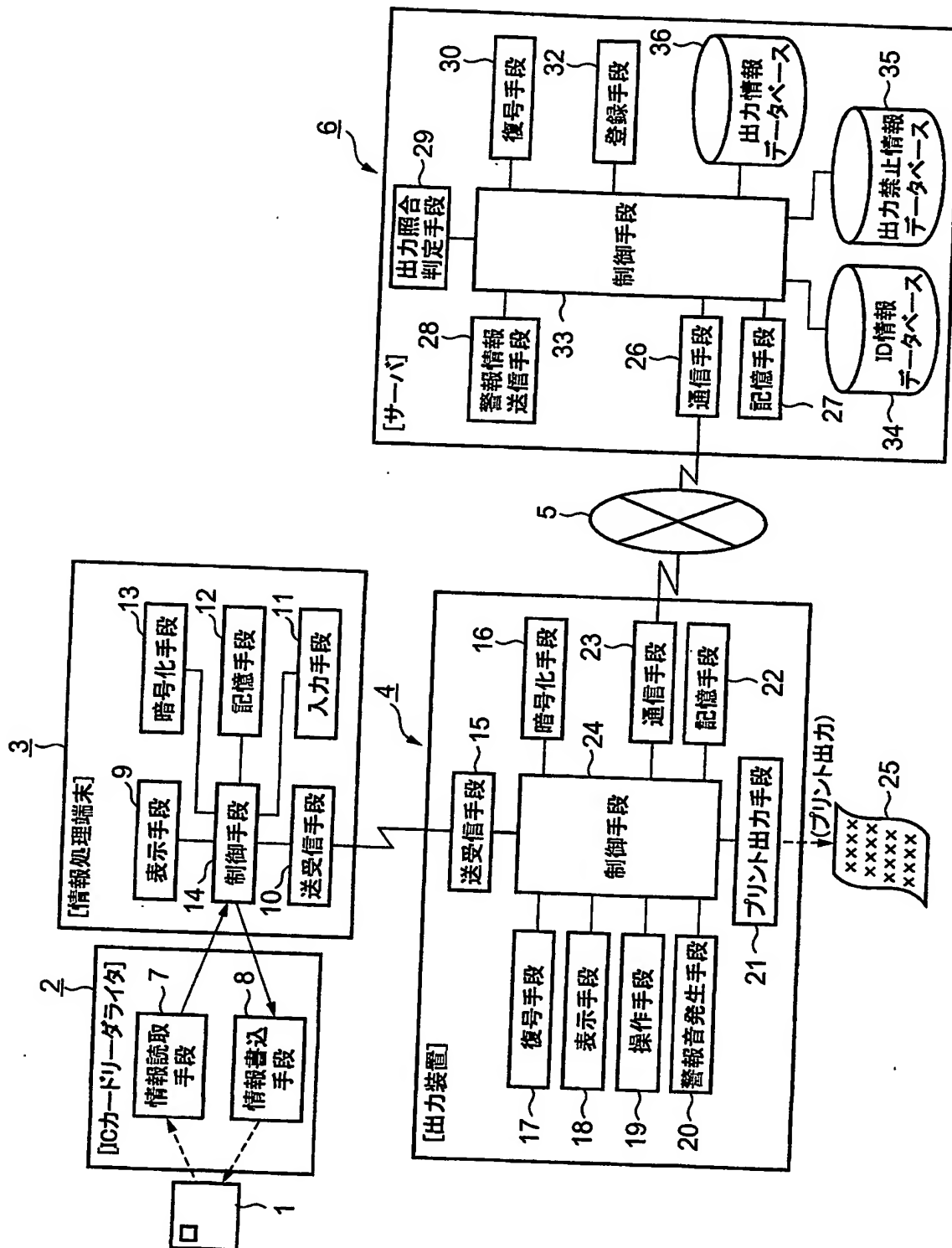
【0027】

- 1 IC カード
- 2 IC カードリーダライタ
- 3 情報処理端末
- 4 出力装置
- 5 通信回線
- 6 サーバ
- 7 情報読取手段
- 8 情報書込手段
- 9 表示手段
- 10, 15 送受信手段
- 11 入力手段
- 12, 22, 27 記憶手段
- 13, 16 暗号化手段
- 14, 24, 33 制御手段
- 17, 30 復号手段
- 19 操作手段
- 20 警報音発生手段
- 21 プリント出力手段
- 23, 26 通信手段
- 25 紙媒体
- 28 警告情報送信手段
- 29 出力照合判定手段
- 32 登録手段
- 34 ID 情報データベース
- 35 出力禁止情報データベース
- 36 出力情報データベース

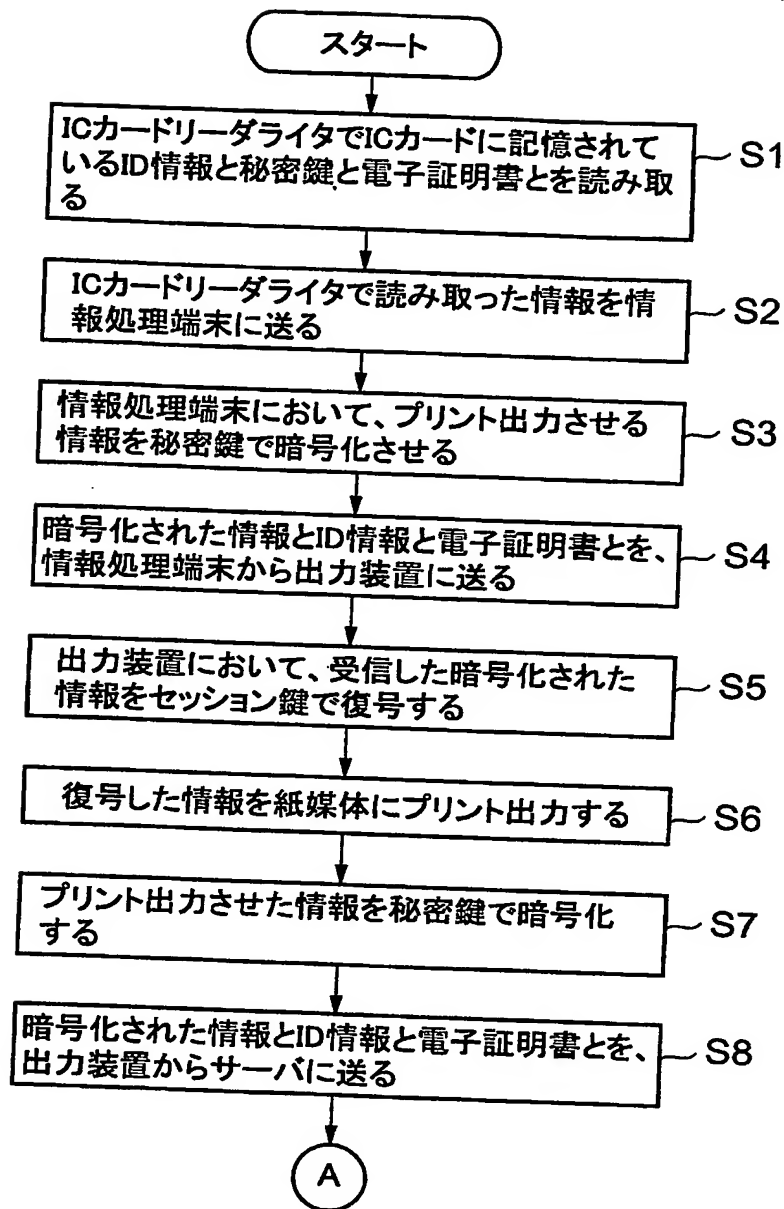
【書類名】 図面
【図 1】



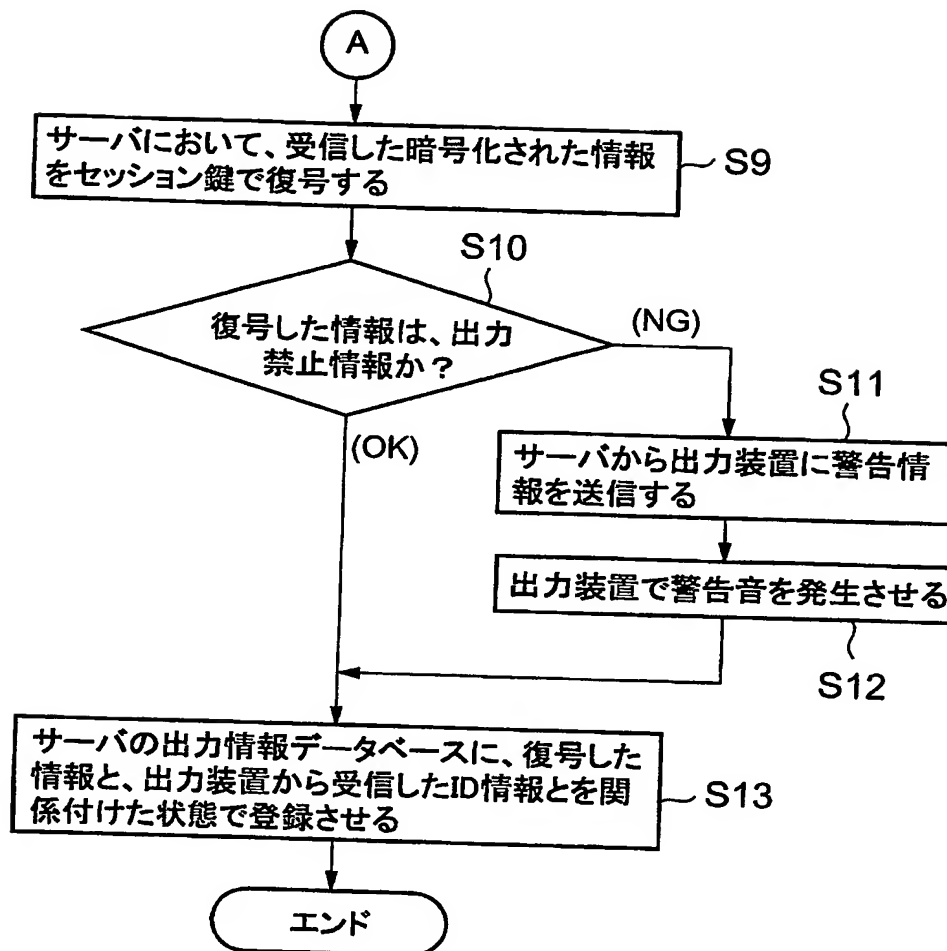
【図 2】



【図 3】



【図 4】



【書類名】要約書

【要約】

【課題】 紙媒体に情報を出力する機能を有する出力装置で、誰が、どのような内容の情報を出力装置で出力したのかに関して具体的な証拠が残るようにした出力情報管理システムを提供する。

【解決手段】 情報記憶媒体と、情報記憶媒体のリーダライタを備えた情報処理端末と、紙媒体に出力する出力装置と、サーバとからなる出力情報管理システムであって、情報記憶媒体は、利用者を特定可能な I D 情報が記憶され記憶手段を有し、リーダライタは、情報記憶媒体に記憶された I D 情報を読み取る読取手段を有し、情報処理端末は、リーダライタで読み取った I D 情報と、出力装置で紙媒体に出力する出力情報とを出力装置に送信する手段とを有し、出力装置は、情報処理端末から受信した I D 情報と出力情報とをサーバに送信する手段を有し、サーバは、出力装置から受信した I D 情報と出力情報とを関係付けてデータベースに記憶させる手段を有することを特徴とする。

【選択図】

図1

特願 2 0 0 4 - 0 5 0 8 4 8

ページ: 1/E

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 2 8 9 7]

1. 変更年月日
[変更理由]

住 所
氏 名

1 9 9 0 年 8 月 2 7 日

新規登録

東京都新宿区市谷加賀町一丁目 1 番 1 号
大日本印刷株式会社